

CLAIMS

1. (Currently Amended) An interactive grid computing system comprising:
a computing service provider side comprising:
 - an interactive grid computing service provider comprising:
 - a grid distributed resource management system (grid DRM)
 - configured for managing a plurality of execution nodes:
 - [[a]] at least one resource that said ~~interactive grid computing service provider~~ DRM reserves for a client based on a request from said client, through a submission node, for an interactive session for a service that said resource is enabled to provide, wherein said at least one resource comprises at least one remote execution node of said plurality of remote execution nodes and at least one fine grained resource, said at least one resource reserved for a requested duration of said interactive session;
 - a first firewall coupled to said at least one resource and configured for protecting said at least one resource, wherein said first firewall is hosting a VNC proxy server; [[and]]
 - a remote display server coupled to said first firewall for providing, at a requested time, secure access, by said submission node, to said at least one resource over a secure connection and for providing interactive graphical data associated with said at least one resource, wherein said client is enabled to communicate directly with said at least one resource over said secure connection during said interactive session ~~wherein said direct communication is not virtual and includes physical data transfer between said client and said resource;~~
 - a software agent associated with said at least one resource, wherein if said at least one resource is requested by said client, said software agent initiates interactive communication between said remote display server and a remote display resource; and
 - a client side coupled to said interactive grid computing service provider, said client side comprising:

a client comprising said remote display resource configured for communicating with said remote display server through said secure connection to access said interactive graphical data provided by said remote display server, wherein said remote display resource is a virtual network computing viewer modified for secure access and for viewing a graphical desktop display associated with said at least one resource, wherein a modification of said virtual network computing viewer comprises:

an established connection between said virtual network computing viewer and said VNC proxy server using a destination host and a destination port address;

a retrieved handle configured for facilitating a creation of a secure socket, said retrieved handle used to create said secure connection through a socks tunnel; and

a second firewall configured for protecting said client, said second firewall hosting a SOCKS proxy server, wherein said secure connection is through said socks tunnel and is used to tunnel said interactive graphical data through said second firewall.

2. (Cancelled)

3. (Cancelled)

4. (Currently Amended) The system as described in Claim [[2]] 1, wherein said remote display resource provides a socksified SSL connection.

5. (Original) The system as described in Claim 1 wherein said interactive graphical data provided by said remote display server is encrypted.

6.-9. (Cancelled)

10. (Original) The system as described in Claim 1 wherein said interactive graphical data is a graphical desktop display associated with said resource.

11. (Original) The system as described in Claim 1 wherein said first firewall comprises a VNC proxy server.

12. (Currently Amended) A method for interactively accessing a remote desktop across a secure network comprising:

receiving a request for ~~[[a]]~~ at least one resource provided by a grid ~~computing application service provider~~ distributed resource management system (grid DRM), said grid DRM configured for managing a plurality of execution nodes, wherein said at least one resource is protected by a first firewall, wherein said at least one resource comprises at least one remote execution node of said plurality of remote execution nodes and at least one fine grained resource, wherein said first firewall comprises a VNC proxy server;

initiating, at a requested time, a remote display server, said remote display server configured for providing interactive graphical data associated with said at least one resource to a remote display viewer, wherein said remote display viewer is protected by a second firewall and is a virtual network computing viewer modified for secure access and for viewing a graphical desktop display associated with said at least one resource, wherein modifying said virtual network computing viewer comprises:

~~protected by a second firewall;~~

establishing a secure socket layer (SSL) connection between said remote display virtual network computing viewer and said remote display VNC proxy server using a destination host and a destination port address, wherein said remote display virtual network computing viewer is enabled to communicate directly with said remote display VNC proxy server;

retrieving a handle that is configured for facilitating a creation of a secure socket;

utilizing said retrieved handle to create said secure connection through a socks tunnel; and

communicating interactive graphical data between said remote display virtual network computing viewer and said remote display VNC proxy server directly

through said SSL connection ~~wherein said communicating is not virtual and includes physical data transfer between said remote display server and said remote display viewer,~~ and wherein said second firewall hosts a SOCKS proxy server, wherein said secure connection is through said socks tunnel and is used to tunnel said interactive graphical data through said second firewall.

13. (Cancelled)

14. (Cancelled)

15. (Currently Amended) The method as described in Claim 12 further comprising receiving said request at said grid DRM ~~computing application service provider~~ from a web browser.

16. (Original) The method as described in Claim 12 further comprising encrypting said graphical data.

17. (Cancelled)

18. (Currently Amended) The method as described in Claim 12 further comprising authenticating a user associated with said ~~remote display~~ virtual network computing viewer.

19. (Original) The method as described in Claim 18 further comprising authenticating said user at an Internet based grid service access point.

20. (Currently Amended) An interactive grid computer system comprising a processor coupled to a bus and a memory coupled to said bus and comprising instructions that when executed implement a method for accessing a remote desktop across firewalls comprising:

receiving a request for ~~[[a]]~~ at least one resource provided by a grid ~~computing application service provider~~ distributed resource management system

(grid DRM), said grid DRM configured for managing a plurality of execution nodes, wherein said at least one resource is protected by a first firewall, wherein said at least one resource comprises at least one remote execution node of said plurality of remote execution nodes and at least one fine grained resource, wherein said first firewall hosts a VNC proxy server;

initiating, at a requested time, a remote display server, said remote display server configured for providing interactive graphical data associated with said at least one resource to a remote display viewer, wherein said remote display viewer is protected by a second firewall and is a virtual network computing viewer modified for secure access and for viewing a graphical desktop display associated with said at least one resource, wherein modifying said virtual network computing viewer comprises:

protected by a second firewall;

establishing a secure socket layer (SSL) connection between said remote display virtual network computing viewer and said remote display VNC proxy server using a destination host and a destination port address, wherein said remote display virtual network computing viewer is enabled to communicate directly with said remote display VNC proxy server;

retrieving a handle that is configured for facilitating a creation of a secure socket;

utilizing said retrieved handle to create said secure connection through a socks tunnel; and

communicating interactive graphical data between said remote display virtual network computing viewer and said remote display VNC proxy server directly through said SSL connection wherein said communicating is not virtual and includes physical data transfer between said remote display server and said remote display viewer, and wherein said second firewall hosts a SOCKS proxy server, wherein said secure connection is through said socks tunnel and is used to tunnel said interactive graphical data through said second firewall.

21. (Cancelled)

22. (Cancelled)

23. (Currently Amended) The interactive grid computer system as described in Claim 20 wherein said method further comprises receiving said request at said grid DRM ~~computing application service provider~~ from an application.

24. (Original) The interactive grid computer system as described in Claim 20 wherein said method further comprises encrypting said graphical data.

25. (Cancelled)

26. (Currently Amended) The interactive grid computer system as described in Claim 20 wherein said method further comprises authenticating a user associated with said ~~remote display~~ virtual network computing viewer.

27. (Original) The interactive grid computer system as described in Claim 20 wherein said method further comprises authenticating said user at an Internet based grid service access point.